**Appeal Brief**
I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with § 1.6(a)(4).

Dated: September 14, 2010
Electronic Signature for Charles A. Bieneman: /Charles A. Bieneman/

Docket No.: 99-703
(PATENT)

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In re Patent Application of:
Sharyn M. Garrity et al.

Application No.: 09/426,442

Confirmation No.: 1897

Filed: October 25, 1999

Art Unit: 2439

For: SYSTEMS AND METHODS FOR SECURING EXTRANET TRANSACTIONS

Examiner: C. J. Brown

# APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir/Madam:

This Appeal Brief is filed pursuant to 37 C.F.R. § 41.37 (a) in furtherance of the Notice of Appeal filed on July 14, 2010. This Appeal Brief appeals the decision of the Examiner in the Final Office Action dated April 14, 2010 ("Final Office Action"), and the Advisory Action dated June 28, 2010 ("Advisory Action"). This application was filed on October 25, 1999.

The fees required under § 41.20(b)(2) are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains items under the following headings as required by 37 C.F.R. § 41.37 and M.P.E.P. § 1205.2:

## TABLE OF CONTENTS

**I. REAL PARTY IN INTEREST ........ 3**

**II. RELATED APPEALS AND INTERFERENCES ........ 4**

**III. STATUS OF CLAIMS ........ 5**

**IV. STATUS OF AMENDMENTS ........ 6**

**V. SUMMARY OF CLAIMED SUBJECT MATTER ........ 7**

**VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL ........ 10**

**VII. ARGUMENT ........ 11**

**CONCLUSION ........ 15**

**APPENDIX A – CLAIMS APPENDIX ........ 16**

**APPENDIX B - EVIDENCE APPENDIX ........ 20**

**APPENDIX C - RELATED PROCEEDINGS APPENDIX ........ 21**

## I. REAL PARTY IN INTEREST

The real party in interest of the present application, solely for purposes of identifying and avoiding potential conflicts of interest by board members due to working in matters in which the member has a financial interest, is Verizon Communications Inc. and its subsidiary companies, which currently include Verizon Business Global, LLC (formerly MCI, LLC) and Cellco Partnership (doing business as Verizon Wirelcss, and which includes as a minority partner affiliates of Vodafone Group Plc). Verizon Communications Inc. or one of its subsidiary companies is an assignee of record of the present application.

## II. RELATED APPEALS AND INTERFERENCES

Appellants (hereinafter "Appellants") are not aware of any related appeals or interferences that would affect the Board's decision on the current appeal. However, the Board is advised of its prior decision in this application, dated May 29, 2009, affirming the Examiner's rejection of claims 1-17 in the Final Office Action dated October 24, 2005. A copy of the Board's May 29, 2009, decision is attached as an Appendix to this Appeal Brief.

## III. STATUS OF CLAIMS

Claims 1, 18-23, 25-33 and 35-37 are pending. Pending claims 1, 18-23, 25-33 and 35-37 are the subject of this appeal, and are reproduced in an Appendix to this brief.

## IV. STATUS OF AMENDMENTS

Appellants amended claims 1, 27 and 37 in their June 11, 2010, Response After Final Action. In the Advisory Action dated June 28, 2010, the Examiner did not state whether these amendments would be entered for purposes of this appeal. (The claims listed in Appendix A include these amendments.)

## V. SUMMARY OF CLAIMED SUBJECT MATTER

The following is a concise explanation of the subject matter defined in at least each of the independent claims involved in the appeal, as required by 37 C.F.R. § 41.37(c)(1)(v). The following explanation is not intended to be used to construe the claims, which are believed to speak for themselves. Nor does Appellant intend the following explanation to modify or add any claim elements, or to constitute a disclaimer of any equivalents to which the claim would otherwise be entitled. Nor is any reference to certain preferred embodiments herein intended to disclaim other possible embodiments.

This summary of the presently claimed subject matter indicates certain portions of the specification (including the drawings) that provide examples of embodiments of elements of the claimed subject mattcr. It is to be understood that other portions of the specification not cited herein may also provide examples of embodiments of elements of the claimed subject matter. It is also to be understood that the indicated examples are merely examples, and the scope of the claimed subject matter includes alternative embodiments and equivalents thereof. References herein to the specification are thus intended to be exemplary and not limiting.

### A. Claim 1

Claim 1 recites an access system for a computer site, comprising:

a certificate authentication component to verify a user's identity from a digital certificate supplied by the user (e.g., Specification, page 9, lines 8-12),

a directory, coupled to the certificate authentication component, to maintain an account for each individual user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access, each account further containing at least one of an internet protocol (IP) address and a ccrtificate authorization method associated with the user (e.g., Specification, page 10, lines 5-14; page 13, lines 4-12; page 21, lines 8-16), and

an access control system, in computer hardware coupled to the directory, for controlling access to computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy associated with the individual user in a directory, wherein the access policy is used to provide tiered access for different sets of users to a plurality of security levels (e.g., Specification, page 6, lines 14-19; page 13, lines 4-12).

**B. Claim 27**

Claim 27 recites a method, comprising:

receiving a request, in computer server hardware, from a user to access a computer site or a portion thereof, the request including information representative of the user's identity (e.g., Specification, page 9, lines 8-12);

verifying the user's identity from the information by consulting a directory that includes accounts for individual users, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access, each account further containing at least one of an internet protocol (IP) address and a certificate authorization method associated with the user (e.g., Specification, page 10, lines 5-14; page 13, lines 4-12; page 21, lines 8-16);

controlling access to the computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy for the user, whercin the access policy is used to provide tiered access for different sets of users to a plurality of security levels (e.g., Specification, page 6, lines 14-19; page 13, lines 4-12).

**C. Claim 37**

Claim 37 recites an access system for a computer site, comprising:

a certificate authentication component to verify a user's identity from a digital certificate supplied by the user (e.g., Specification, page 9, lines 8-12),

a directory, coupled to the certificatc authentication component, to maintain an account for each individual user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access, each account further containing at least one of an internet protocol (IP) address and a certificate authorization method associated with the user (e.g., Specification, page 10, lines 5-14; page 13, lines 4-12; page 21, lines 8-16), and an access control system, in computer hardware coupled to the directory, for controlling access to computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy associated with the individual user in a directory, wherein the access policy is used to provide tiered access for different sets of users to a plurality of security levels (e.g., Specification, page 6, lines 14-19; page 13, lines 4-12);

and further wherein the access control system is configured to use information relating to the user to present to the user personalized information, the information relating to the user being at least one of the user's navigation history and the user's preferences, and the personalized information being at least one of information relating to new products and developments in the user's field of interest (e.g., Specification, page 14, line 22 – page 15, line 12).

## VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The Final Office Action set forth the following grounds for rejecting Appellant's claims, which grounds are to be reviewed in this appeal:

1. That claims 1, 27, and 37 are allegedly directed to non-statutory subject matter and are therefore unpatentable under 35 U.S.C. §101;

2. That claims 1, 19, 20, 24, 25-27, 29, 30, 34, 35, and 36 are allegedly unpatentable under 35 U.S.C. § 103(a) over United States Patent No. 6,367,009 ("Davis") in view of United States Patent No. 6,178,505 ("Schneider") in view of United States Patent No. 6,023,765 ("Kuhn");

3. That claims 21, 22, 31, 32, and 37 are allegedly unpatentable under 35 U.S.C. § 103(a) over Davis in view of the Schneider and Kuhn and further in view of United States Patent Application No 2001/0020242 ("Gupta"); and

4. That claims 18, 23, 28, and 33 are allegedly unpatentable under 35 U.S.C. § 103(a) over Davis in view of Schneider and Kuhn and further in view of United States Patent No. 6,240,091 ("Ginzboorg").

## VII. ARGUMENT

### A. GROUND OF REJECTION NO. 1 (Claims 1 and 18-37)

The Examiner rejected each of independent claims 1, 27, and 37 under Section 101 "because they do not contain any form of computer hardware." (Office Action, page 3.) To expedite prosecution, Appellants followed the Examiner's suggestion at page 3 of the Office Action and, in their After Final response dated June 11, 2010, amended the independent claims to explicitly include the word "hardware." In the Advisory Action dated June 28, 2010, the Examiner did not indicate whether these amendments were entered. If these amendments were entered, Appellants respectfully submit that the Examiner's Answer should withdraw the Section 101 rejection of the claims before this application is sent to the Board, and that, otherwise, that rejection should be reversed for at least the following reason.

Because these claims recited a "computer" even prior to Appellants' June 11, 2010, paper, the claims were clearly drawn to a machine and not to an abstract idea. Therefore, even if Appellants' amendments of June 11, 2010, were not entered, the Section 101 rejection of the claims should be reversed.

### B. GROUND OF REJECTION NO. 2 (Claims 1, 19, 20, 24, 25-27, 29, 30, 34, 35, and 36)

Independent claim 1, rejected as allegedly unpatentable over Davis in view of Schneider and further in view of Kuhn, recites in part:

> a directory, coupled to the certificate authentication component, to maintain an account for each individual user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access, <u>each account further containing at least one of an internet protocol (IP) address and a certificate authorization method associated with the user</u>.

The Examiner alleged that "Schneider teaches a user account with an associated IP address." (Office Action, page 4.) However, while Schneider does discuss Internet protocol (IP) addresses, Schneider does not teach or suggest "each account further containing . . . an Internet protocol (IP) address," much less "an internet protocol (IP) address . . . associated with the user." Further, contrary to the Examiner's allegations (*id.*, page 2), Schneider does not teach or suggest an account containing "a certificate authorization method associated with the user," as recited in claim 1.

Schneider discloses "access filters" that use techniques "to determine the minimum amount [of security needed by a session]." (Schneider, column 18, lines 23-25.) When an access filter is implemented, a "trust level for a user is determined from the manner in which [an] access request identifies the user." (*Id.,* column 18, lines 59-60.) Thus, an access filter may include a table containing, among other things, "minimum identification methods." (*Id.,* column 19, lines 48-50.) One way for the user to be identified from an access request is by "the IP address or fully qualified domain name of the user's computer." (*Id.,* column 19, lines 19-20.) In other words, Schneider teaches at most that IP addresses may be included in access filters, but Schneider's access filters are not associated with individual users. Moreover, the tables in Schneider's access filters are not associated with individual users, and are not in any way user accounts. In short, Schneider in no way teaches or suggests "an account for each individual user" that contains "an Internet protocol (IP) address . . . associated with the user."

Consistent with his teachings regarding access filters, Schneider teaches that user IP addresses may be provided at most from user session information, and not from a user account. That is, Schneider discloses that users may be "identified by IP addresses" and may "appear in [a] display as ranges of IP addresses." (*Id.,* column 23, lines 18-20.) Then, "users whose sessions have the source IP addresses listed" in the display may be added to a user group. (*Id.,* column 23, lines 30-33.) Thus, a user session, and not a user account, provides a user IP address in Schneider.

The Examiner responded to the foregoing arguments, first made in Appellants' January 22, 2010, paper, by asserting that "Schneider teaches a 'range' of IP addresses for each user." (Office Action, page 2.) Then the Examiner asserted, without any support, "that this still associates an IP address for a user." In short, the Examiner has admitted that Schneider does not disclose "an Internet protocol (IP) address . . . associated with the user," and the Examiner has moreover admitted, at least implicitly, that Schneider does not even teach or suggest "a user account" with which an IP address could be associated. For at least these reasons, the present rejection of claim 1 must be reversed.

Further, the Examiner's response to the above argument that Schneider's "access filters" do not amount to "an Internet protocol (IP) address . . . associated with the user" was to assert that "Schneider teaches users are defined in 'information sets' in a database." (Office Action, page 2.)

The Examiner further contended that "user information data sets 313" read on the "account" recited in claim 1. However, Schneider's "information sets" are not in fact user account data but rather are business data to which users have access according to an access policy. (*See, e.g.,* Schneider, column 12, lines 21-53.) Moreover, Schneider discloses simply that "[d]atabase 301 permits hierarchical definition of both user groups and information sets." As discussed above, user groups may be subject to access filters, but users are not identified according to IP addresses. Indeed, Schneider discloses a number of modes for identifying and authenticating a user, but none of these include associating a user with an IP address. (*See* Schneider, column 13, lines 1-28.) For at least these further reasons, the present rejection of claim 1 must be reversed.

The Examiner also stated that he did "not believe the argument about sessions is relevant." (Office Action, page 2.) According to the Examiner, "[t]he session IP address, which is also the IP address of the user, has previously been stored in a database that identifies the user, and then that user has been assigned to a group." (Office Action, page 2.) Appellants respectfully disagree that Schneider includes such a teaching or suggestion, or that such a teaching or suggestion applies to Appellants' claims. Notably, the Examiner has not identified the portion or portions of Schneider that allegedly discloses storing a session IP address associated with a user in a database. Indeed, a user session providing an IP address to be compared against a range of IP addresses in an access filter would have meant that there was no need to store a particular user's IP address because the IP address was obtained from the user session. For at least these further reasons, the rejection of claim 1 must be reversed.

The Examiner has also argued that, alternatively, "Schneider also teaches that the database contains a certificate authorization method associated with the user as shown in Column 11 lines 1-55 (matching)." (Office Action, page 2.) However, Schneider simply teaches a certificate authorization method in which a certificate may include a description of a hypothetical user who may access certain data. Schneider's user groups may be defined according to "certificate matching criteria which define the values of the fields which a certificate that belongs to a member of a given user group must have." (Schneider, column 11, lines 52-56.) Schneider does not include any teaching or suggestion of a "certificate authorization method associated with the user" because Schneider teaches at most matching certificates to user groups, not users. Further, Schneider merely teaches such "matching" and does not teach or suggest that the user groups include a "certificate authorization method." In short, Schneider in no way teaches or suggests "an account for each individual user" that includes a "certificate authorization method associated with the user" as required by claim 1. For at least these further reasons, the Examiner's rejection must be reversed.

In sum, Schneider does not teach or suggest "each account further containing at least one of an Internet protocol (IP) address and a certificate authorization method associated with the user," as recited in claim 1. Neither Davis nor Kuhn compensates for the deficiencies of Schneider. Therefore, claim 1, and all claims depending therefrom, are in condition for allowance over the cited references at least for the foregoing reasons.

Independent claims 27 and 37 both recite "each account further containing at least one of an Internet protocol (IP) address and a certificate authorization method associated with the user." Therefore, these claims, and the claims depending from claim 27, are likewise in condition for allowance over the cited references at least for the foregoing reasons.

### C. GROUND OF REJECTION NO. 3 (Claims 21, 22, 31, 32, and 37)

Each of claims 21, 22, 31, 32, and 37 is patentable at least by reason of dependence from one of independent claims 1 or 17, and therefore the rejection of these claims must be reversed.

### D. GROUND OF REJECTION NO. 4 (Claims 18, 23, 28, and 33)

Each of claims 21, 22, 31, 32, and 37 is patentable at least by reason of dependence from one of independent claims 1 or 17, and therefore the rejection of these claims must be reversed.

## CONCLUSION

In view of the foregoing arguments, Appellant respectfully submits that the pending claims are novel over the cited references. The Examiner's rejections of all pending claims are improper because the references do not teach or suggest each and every element of the claimed invention. In view of the above analysis, a reversal of the rejections of record is respectfully requested of this Honorable Board.

It is believed that any fees associated with the filing of this paper are identified in an accompanying transmittal. However, if any additional fees are required, they may be charged to Deposit Account 18-0013, under Order No. 65632-0632, from which the undersigned is authorized to draw. To the extent necessary, a petition for extension of time under 37 C.F.R. 1.136(a) is hereby made, the fee for which should be charged against the aforementioned account.

Dated: September 14, 2010

Respectfully submitted,

Electronic signature: /Charles A. Bieneman/
Charles A. Bieneman
Registration No.: 51,472
Michael B. Stewart
Registration No.: 36,018
RADER, FISHMAN & GRAUER PLLC
Correspondence Customer Number: 25537
Attorneys for Applicant

## APPENDIX A – CLAIMS APPENDIX

Pursuant to 37 C.F.R. § 41.37(c)(vii), the following listing provides a copy of the claims involved in this appeal.

1. An access system for a computer site, comprising:

a certificate authentication component to verify a user's identity from a digital certificate supplied by the user,

a directory, coupled to the certificate authentication component, to maintain an account for each individual user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access, each account further containing at least one of an internet protocol (IP) address and a certificate authorization method associated with the user, and

an access control system, in computer hardware coupled to the directory, for controlling access to computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy associated with the individual user in a directory, wherein the access policy is used to provide tiered access for different sets of users to a plurality of security levels.

18. The access system of claim 1, further comprising a digital signing module that produces and stores at least one of a digital signature and a timestamp for a transaction.

19. The access system of claim 1, wherein users are categorized into discrete sets, and each set is granted access to a particular portion of the computer site according to the access policy.

20. The access system of claim 1, the system configured to use information relating to the user to present to the user personalized information.

21. The access system of claim 20, wherein the information relating to the user is at least one of the user's navigation history and the user's preferences.

22. The access system of claim 20, wherein the personalized information is at least one of information relating to new products and developments in the user's field of interest.

23. The access system of claim 1, the system configured to maintain an archive relating to the account, the archive including information relating to at least one of purchases made, available credit, applicable discounts, and links to specific recorded transactions.

25. The access system of claim 1, the system being configured for supporting desired functionality of designated users.

26. The access system of claim 1, further comprising an automation component to permit automation of certificate authorization.

27. A method, comprising:

receiving a request, in computer server hardware, from a user to access a computer site or a portion thereof, the request including information representative of the user's identity;

verifying the user's identity from the information by consulting a directory that includes accounts for individual users, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access, each account further containing at least one of an internet protocol (IP) address and a certificate authorization method associated with the user;

controlling access to the computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy for the user, wherein the access policy is used to provide tiered access for different sets of users to a plurality of security levels.

controlling access to the computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy associated with the user.

28. The method of claim 27, further comprising producing and storing at least one of a digital signature and a timestamp for a transaction.

29. The method of claim 27, further comprising categorizing users into discrete sets, and granting each set access to a particular portion of the computer site according to the access policy.

30. The method of claim 27, further comprising using information relating to the user to present to the user personalized information.

31. The method of claim 30, wherein the information relating to the user is at least one of the user's navigation history and the user's preferences.

32. The method of claim 30, wherein the personalized information is at least one of information relating to new products and developments in the user's field of interest.

33. The method of claim 27, further comprising maintaining an archive relating to the account, the archive including information relating to at least one of purchases made, available credit, applicable discounts, and links to specific recorded transactions.

35. The method of claim 27, further comprising supporting desired functionality of designated users.

36. The method of claim 27, further comprising automating certificate authorization.

37. An access system for a computer site, comprising:

a certificate authentication component to verify a user's identity from a digital certificate supplied by the user,

a directory, coupled to the certificate authentication component, to maintain an account for each individual user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access, each account further containing at least one of an internet protocol (IP) address and a certificate authorization method associated with the user, and

an access control system, in computer hardware coupled to the directory, for controlling access to computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy associated with the individual user in a directory, wherein the access policy is used to provide tiered access for different sets of users to a plurality of security levels;

and further wherein the access control system is configured to use information relating to the user to present to the user personalized information, the information relating to the user being at least one of the user's navigation history and the user's preferences, and the personalized information being at least one of information relating to new products and developments in the user's field of interest.

## APPENDIX B - EVIDENCE APPENDIX

Not applicable – in this Appeal, Appellant does not rely on any evidence submitted pursuant to 37 CF.R.F. §§ 1.130, 1.131, or 1.132, or on any other evidence entered by the Examiner.

## APPENDIX C - RELATED PROCEEDINGS APPENDIX

A copy of the Board's decision, dated May 29, 2009, on the prior appeal in this matter, is attached.

UNITED STATES PATENT AND TRADEMARK OFFICE

---

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

---

*Ex parte* SHARYN MARIE GARRITY, RONALD LEWIS SCOTT, and
AARON MARK HELSINGER

---

Appeal 2008-004379
Application 09/426,442
Technology Center 2400

---

Decided:[1] May 29, 2009

---

Before JAMES D. THOMAS, LEE E. BARRETT, and STEPHEN C. SIU, *Administrative Patent Judges.*

SIU, *Administrative Patent Judge.*

# DECISION ON APPEAL

[1] The two month time period for filing an appeal or commencing a civil action, as recited in 37 C.F.R. § 1.304, begins to run from the decided date shown on this page of the decision. The time period does not run from the Mail Date (paper delivery) or Notification Date (electronic delivery).

## STATEMENT OF THE CASE

This is a decision on appeal under 35 U.S.C. § 134(a) from the Examiner's rejection of claims 1–17. We have jurisdiction under 35 U.S.C. § 6(b).

We affirm.

### *Invention*

The invention relates to providing secure access and transactions using a certificate authentication component to verify a user's identity, a directory to store an access policy for each user, and an access control system to restrict access to users based on the access policy information associated with each user (Spec. 3, ll. 4–13).

Independent claim 1 is illustrative:

> 1. An access system for a computer site, comprising a certificate authentication component to verify a user's identity from a digital certificate supplied by the user,
>
> a directory, coupled to the certificate authentication component, to maintain an account for each individual user, each account containing an access policy specifying at least one portion of the computer site to which the corresponding user is permitted access, and
>
> an access control system, coupled to the directory, for controlling access to a computer site by permitting the user to access a portion of the computer site and restricting the user from accessing at least one other portion of the computer site, based on the access policy associated with the individual user in a directory.

### *References*

The Examiner relies upon the following references as evidence in support of the rejections:

| | | |
|---|---|---|
| Davis | US 6,367,009 B1 | Apr. 2, 2002<br>(filed Dec. 17, 1998) |

| | | |
|---|---|---|
| Ginzboorg | US 6,240,091 B1 | May 29, 2001<br>(filed Oct. 17, 1997) |
| Bertram | US 5,948,064 | Sep. 7, 1999 |
| Grimmer | US 5,774,552 | Jun. 30, 1998 |

*Rejection*

The Examiner rejects claims 1, 2, and 7–14 under 35 U.S.C. § 103(a) as being unpatentable over Davis in view of Bertram, claims 4–6, 16, and 17 under 35 U.S.C. § 103(a) as being unpatentable over Davis in view of Bertram and Ginzboorg, and claims 3 and 15 under 35 U.S.C. § 103(a) as being unpatentable over Davis in view of Bertram and Grimmer.

*Appellants' Contentions*

Appellants urge reversal, arguing there is no motivation to combine Davis and Bertram (App. Br. 13–14).

*Examiner's Findings/Conclusions*

The Examiner disagrees, averring that it would have been obvious to one of ordinary skill in the art to combine Davis and Bertram (Ans. 6).

## ISSUE

Have Appellants shown that the Examiner erred in concluding that it would have been obvious to one of ordinary skill in the art to combine Davis and Bertram?

## FINDINGS OF FACT

The following Findings of Fact (FF) are shown by a preponderance of the evidence.

1. Davis teaches how to enable "the true client's identity to be known to the application on the end-tier server" (Abstract).

2. Davis teaches that "The manner in which the application program uses the name is application dependent, and does not form part of the present invention. As an example of the application-dependent processing, if access control is being used on the ETS as previously described, the application program will compare this name to its list (or other representation) of authorized users. If the name is authorized, then the application will process the request that is being made on behalf of the first-tier client; otherwise, the request will be rejected" (col. 13, ll. 33–42).

3. Bertram teaches "a discovery 'policy' to tailor the way in which a user may access and interact with the discovered information" (Abstract).

4. Bertram teaches that "authentication is a process is [*sic*] which the userid and password are provided to a user account database for validation. Upon successful validation, a positive confirmation is received for the authentication and the user processing is allowed to continue" (col. 6, ll. 1–5).

## PRINCIPLES OF LAW

### *Obviousness*

> Section 103(a) forbids issuance of a patent when "the
> differences between the subject matter sought to be patented
> and the prior art are such that the subject matter as a whole
> would have been obvious at the time the invention was made to
> a person having ordinary skill in the art to which said subject
> matter pertains."

*KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 406 (2007).

"What matters is the objective reach of the claim. If the claim extends to what is obvious, it is invalid under § 103." *Id.* at 419. In *KSR*, the Supreme Court emphasized "the need for caution in granting a patent based on the combination of elements found in the prior art," *id.* at 415, and discussed circumstances in which a patent might be determined to be obvious. *Id.* at 415–16 (citing *Graham v. John Deere Co.*, 383 U.S. 1, 12 (1966)). The Court reaffirmed principles based on its precedent that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Id.* at 416. The operative question in this "functional approach" is thus "whether the improvement is more than the predictable use of prior art elements according to their established functions." *Id.* at 415, 417.

The Federal Circuit recognizes that "[a]n obviousness determination is not the result of a rigid formula disassociated from the consideration of the facts of a case. Indeed, the common sense of those skilled in the art demonstrates why some combinations would have been obvious where others would not." *Leapfrog Enters., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1161 (Fed. Cir. 2007) (citing *KSR*, 127 S. Ct. 1727, 1739 (2007)). The Federal Circuit relied in part on the fact that Leapfrog had presented no evidence that the inclusion of a reader in the combined device was "uniquely challenging or difficult for one of ordinary skill in the art" or "represented an unobvious step over the prior art." *Id.* at 1162 (citing *KSR*, 127 S. Ct. at 1740–41).

## ANALYSIS

We concur with the Examiner's finding that it would have been obvious to one of ordinary skill in the art to combine Davis and Bertram. Davis teaches how to identify who or what is trying to connect to a protected system (FF 1). Bertram teaches the use of user accounts to establish access control policies for protected systems (FF 3–4). These are complementary teachings, both being used according to their established functions to yield a predictable result. *See KSR*, 550 U.S. at 417.

Appellants have not shown that it would have been uniquely challenging or difficult for one of ordinary skill in the art to combine Davis and Bertram. *See Leapfrog Enters., Inc.*, 485 F.3d at 1162. Nor have Appellants shown that the invention represents an unobvious step over Davis and Bertram. *Id.*

Furthermore, the Examiner recognized that one of ordinary skill in the art would have been motivated to look to what was known outside of Davis to improve its "security and flexibility" (Ans. 4). Davis presented a simple access control policy example: a list of authorized users. But Davis made clear that access control policies were not part of the invention (FF 2). One of ordinary skill in the art would look to other authentication teachings, such as Bertram (FF 4), to find access control policy teachings more robust than the example described in Davis.

For at least these reasons, we conclude that Appellants have not sustained the requisite burden on appeal in providing arguments or evidence persuasive of error in the Examiner's rejection of claims 1, 2, and 7–14. Appellants make no new arguments in support of claims 3–6 and 15–17, thus we further conclude that Appellants have not shown error in the Examiner's rejection of these claims.

## CONCLUSIONS OF LAW

Based on the findings of facts and analysis above, we conclude that Appellants have failed to demonstrate that the Examiner erred in finding that it would have been obvious to one of ordinary skill in the art to combine Davis and Bertram.

## DECISION

We affirm the Examiner's decision rejecting claims 1–17.

## AFFIRMED

erc

VERIZON LEGAL DEPARTMENT
PATENT MANAGEMENT GROUP
1320 N. COURTHOUSE ROAD
9TH FLOOR
ARLINGTON, VA 22201-2525